REMARKS/ARGUMENTS

The Examiner rejects claims 31, 40, and 18 under 35 U.S.C.§112, first paragraph, as failing to comply with the enablement requirement. According to the Examiner, the "claim(s) contain subject matter such as ". . . members . . ." which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention."

Applicants disagree. The use of the word "members" and "memberships" describes, for example, the transmission of RTP and RTCP packets to the other endpoint and RTCP packets only to the session monitor.

With this in mind, the specification states at page 1, lines 9-21, as follows:

> Real Time Protocol ("RTP") is the standard protocol defining the real-time transmission of media streams (*e.g.*, voice) over data networks, such as in Voice Over IP. A companion protocol to RTP is the Real Time Control Protocol or RTCP. *Referring to Fig. 1, media packets transmitted between A 100 and B 104 and vice versa during a session are formatted and transmitted (continuously) over network 108 according to RTP while additional performance information governing the communication link (e.g., key statistics about the media packets being sent and received by each endpoint (A or B) such as jitter, packet loss, round-trip time, etc.) are transmitted (discontinuously) over the network 108 according to RTCP.* Endpoints A and B are typically computational components but can be or include any other form of audio or video communications interface. RTCP performance information is useful not only for the session participants, A and B, but also for a network monitor 112. Network administrators can use such information not only for network administration but also for network troubleshooting and management.

(Emphasis supplied.)

The Specification further states at page 2, line 13, to page 3, line 9, as follows:

> To enable the monitor to obtain RTCP packets, a dual unicast architecture has been developed. *In dual unicast, one session participant (A) transmits both RTP and RTCP packets to the other session participant (B) and RTCP packets to the monitor.* Dual unicast, however, exposes design limitations in the RTCP protocol itself. Although endpoint session ids are unique to a particular (first) session (such as between A and B), an endpoint in a concurrent (second) session (such as between C and D) can have the

same session id or synchronization source id ("SSRC") as an endpoint (A or B) in the other (first) session. When duplicate endpoint session ids are concurrently in use, the monitor can have substantial difficulty determining which RTCP packets correspond to which session, potentially causing inaccurate performance analysis.

By way of illustration, in the example above assume that A sends an RTCP packet addressed to B and an RTCP packet addressed to the monitor. The RTCP packet addressed to the monitor includes A's transport address, A's SSRC, and B's SSRC but does not include the transport address of B. Likewise, C sends an RTCP packet addressed to D and an RTCP packet addressed to the monitor. The RTCP packet addressed to the monitor includes C's transport address, C's SSRC, and D's SSRC but does not include the transport address of D. If B and D have the same SSRC, the monitor is unable to definitively determine that a selected RTCP packet sent to either B or D corresponds to the A-B session or the C-D session.

(Emphasis supplied.)

The specification further states at page 10, line 20, to page 11, line12, as follows:

Fig. 4 depicts the algorithm for a computational component in the first endpoint that is configured to input another (second) endpoint's SSRC id into the APP field. In step 400, the first endpoint receives an RTCP packet from the second endpoint participating in a session with the first endpoint. *In step 404, the first endpoint parses the RTCP packet and determines whether a flag has been set (i.e., determines the flag's value). The flag identifies whether or not the second endpoint is configured to transmit a duplicate packet to the session monitor. If the flag is set (meaning that the second endpoint is configured to transmit a duplicate packet to the session monitor), the first endpoint in step 408 does not forward a modified version of the RTCP packet to the monitor.* The first endpoint returns to step 400 to await the next RTCP packet. *If the flag is not set (meaning that the second endpoint is not configured to send a duplicate RTCP packet to the monitor), the first endpoint in step 412 modifies the RTCP packet by replacing the destination address with that of the monitor and inputs into the APP field the second endpoint's network address and forwards the modified packed to the monitor 300.* The forwarding can be done by any suitable technique such as port forwarding.

(Emphasis supplied.)

As can be seen from the above excerpts, the specification clearly disclosed (a) the transmission, by one endpoint, to another endpoint of both RTP and RTCP packets (which

contain different information) and RTCP packets only to the session monitor and (b) when dual unicast is not in use, the transmission, by one endpoint, to the other endpoint of outgoing RTP and RTCP packets and incoming (from the other endpoint) RTCP packets to the session monitor. This disclosure supports, for example, the claimed phrase:

> a first endpoint transmitting first and second sets of packets, respectively, to a session monitor and a second endpoint, wherein the first and second sets of packets have differing memberships, wherein each packet in the first set of packets is used for determining network performance information

In one construction of this phrase, the "first" set of packets includes RTCP packets only while the "second" set of packets includes both RTP and RTCP packets. Thus, the first and second sets have differing packet memberships.

The Examiner rejects claims 31-56 under 35 U.S.C.§102(e) as being anticipated by Pruthi, et al., (U.S. 2002/0105911) ("Pruthi").

Applicant respectfully traverses the Examiner's rejections. Pruthi fails to teach or suggest at least the following italicized features of the pending independent claims:

> 31. A method for identifying a corresponding session for a packet, comprising:
> (a) in a first session, *a first endpoint transmitting first and second sets of packets, respectively, to a session monitor and a second endpoint, wherein the first and second sets of packets have differing memberships, wherein each packet in the first set of packets is used for determining network performance information, and wherein each of the first and second endpoints have an associated electronic address on a network and a session identifier*;
> (b) the session monitor receiving at least a first packet in the first packet set, the first packet comprising at least the network address and session identifier associated with the first endpoint;
> (c) determining whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a first set of data structures, *the first set of data structures comprising active session entries, each entry in*

the first set of data structures having at least network addresses for each of the endpoints to the corresponding session;

(d) *when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the first set of data structures*, updating the corresponding entry to include the network performance information associated with the at least a first packet;

(e) *determining whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a second set of data structures, the second set of data structures having active session entries, each of the entries in the second set of data structures failing to comprise network addresses for each of the endpoints to the corresponding session*; and

(f) *when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the second set of data structures*, updating the entry to include the performance information associated with the at least a first packet.

40. In a network, the network comprising:

(i) a session monitor operable to track network performance for a plurality of sessions; and

(ii) *first endpoint and second endpoints, the first endpoint being operable to transmit first and second sets of packets, respectively, to the session monitor and the second endpoint, wherein the first and second sets of packets have differing memberships, wherein each packet in the first set of packets is used by the session monitor to determine network performance information, and wherein each of the first and second endpoints have an associated electronic address on a network and a session identifier*, the session monitor comprising:

(a) an input operable to receive at least a first packet in the first packet set, the first packet comprising at least the network address and session identifier associated with the first endpoint; and

(b) a matcher operable to:

(b1) determine whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a first set of data structures, *the first set of data structures comprising active session entries, each entry in the first set of data structures having at least network addresses for each of the endpoints to the corresponding session*;

(b2) *when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the first set of data structures,* update the corresponding entry to include the performance information associated with the at least a first packet;

(b3) *determine whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a second set of data*

structures, the second set of data structures having active session entries, each of the entries in the second set of data structures failing to comprise network addresses for each of the endpoints to the corresponding session; and

(b4) *when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the second set of data structures,* update the entry to include the performance information associated with the at least a first packet.

48. In a network, the network comprising:

(i) a session monitor operable to track network performance for a plurality of sessions; and

(ii) first endpoint and second endpoints, *the first endpoint being operable to transmit first and second sets of packets, respectively, to the session monitor and the second endpoint, wherein the first and second sets of packets have differing memberships, wherein each packet in the first set of packets is used by the session monitor to determine network performance information, and wherein each of the first and second endpoints have an associated electronic address on a network and a session identifier*, a method comprising:

(a) the first endpoint receiving at least a first packet communicated between the first endpoint and a second endpoint to a first session, the first packet comprising an address of the first endpoint on the network, an address of the second endpoint on the network, *and voice information*, and *being a member of the second packet set*; and

(b) *the first endpoint transmitting at least a second packet to a session monitor, the at least a second packet including the respective first and second network addresses of the first and second endpoints and being a member of the first packet set.*

51. In a network, the network comprising:

(i) a session monitor operable to track network performance for a plurality of sessions; and

(ii) first endpoint and second endpoints, *the first endpoint being operable to transmit first and second sets of packets, respectively, to the session monitor and the second endpoint, wherein the first and second sets of packets have differing memberships, wherein each packet in the first set of packets is used by the session monitor to determine network performance information, and wherein each of the first and second endpoints have an associated electronic address on a network and a session identifier*, the first endpoint comprising:

(a) an input operable to receive at least a first packet communicated between the first and second endpoints to a first session, the first packet comprising a network address of the first endpoint, a network address of the second endpoint, and voice information, and being a member of the second packet set; and

(b) *a transmitter operable to transmit at least a second packet to a session monitor, the at least a second packet including the respective first and second network addresses of the first and second endpoints and being a member of the first packet set.*

54. A session packet for transmission on a network, comprising:
a source network address of a first participant to a *Voice over Internet Protocol (VoIP) session*;
a destination network address associated with a session monitor;
a network address of a second participant to the VoIP session; and
session information associated with the VoIP session.

In one embodiment, the present addresses this problem by maintaining a listing of network addresses and/or session identifiers to track active RTP sessions. When an RTCP packet is received, the network address and/or session identifier of the source endpoint matches an entry in the listing, a network address of the destination endpoint is determined. The listing can cause the window of opportunity for confusing concurrent sessions and attributing data in RTCP packets to the wrong session to be much smaller than with current architectures. The window of opportunity for possible confusion using the above algorithm(s) exists only when two different endpoints join different sessions at the same time and with the same SSRC ids. This window of opportunity or startup interval closes once either of the endpoints (or their peers) has sent an RTCP packet with a reception block corresponding to either endpoint. Once the reception block is exchanged, the SSRC ids of both parties to the session are known to the monitor. Before such an exchange, the monitor typically has only the SSRC id and network address of one party to the session. The SSRC id and network address of the other party is unknown. The startup interval is typically fairly short, *e.g.*, typically on the order of 5 seconds or less. The use of the active session table and network address to define the session (rather than only pairings of SSRC ids) can, after the startup interval, at least substantially eliminate misinterpretation of RTCP packets and incorrect analysis of performance data. The accuracy of the algorithm(s) in matching RTCP packets with the corresponding session results in more accurate statistical analysis of the communication link in the network.

Pruthi et al. is directed to a method for monitoring data on a first communication line. Data is received from the first communication line and a plurality of packets are extracted from the data. Statistics are then recursively generated, the statistics corresponding to the plurality of packets.

As shown in Figure 1, the network monitor 102 is coupled to the network N1106 via a first communication line 104. The monitor receives (monitors) data communications (traffic) on communication line 104 and provides real-time metrics or statistics of the data traffic on the communication line 104.

Packets are extracted from the bit stream and converted into records stored in memory. The records are generated by first determining the type (protocol or layer) of each packet (step 414) and then filtering the packets (step 416) based on their determined types. An index is generated (step 418) for each packet and the packet is then converted into an indexed record (step 420) and stored in memory (step 422). The time when the network monitor received each IP packet is used as an index for each IP packet.

Exemplary information retained respecting each packet includes the type of the packet, the size of the packet, a packet number, an interface number, an application, and an associated session. Further statistics are then generated (step 426) using the statistics previously generated for the packets and records are then provided to one or more applications such as a display device (step 428), a router for dynamically adjusting network routing based on the further statistics (step 430), and a billing service for billing clients based on quality or quantity of service as determined based on the generated statistics (step 432). Alternatively, the record may include a plurality of fields, each corresponding to a portion of the IP packet such as a source address or destination address, and filtering may be performed based on any one or more of the plurality of fields. Statistics measured include packet size distributions, protocol distributions, bandwidth usage per client, bandwidth usage by domain, average response time per server, average round-trip time

between server-client pair, and performance metrics (e.g., the ratio of the number of bits in IP packets received to the number of bits in all packets received for each successive minute, and).

It is not clear in Pruthi et al. how packets are paired up with sessions. In an example at ¶¶ 0047 and 0048, ATM session packets are apparently matched by ATM session identifier alone. Pruthi et al. further fails to teach the use of first and second sets of data structures to contain network performance information respecting unidentified and identified sessions, respectively. Additionally, Pruthi et al. fails to teach dual unicasting in which separate packets are transmitted to the other endpoint and a performance monitor. Rather, Pruthi et al. teaches away from dual unicasting. Pruthi et al. teaches the extraction of packets being exchanged between session endpoints to avoid intruding into the network to evaluate or estimate network performance. According to Pruthi et al., intrusion by introducing additional packets into the network can further degrade performance. (¶0008.)

Accordingly, the pending claims are allowable.

The dependent claims provide further reasons for allowance.

Dependent claims 32 and 41 require the first set of packets to include fewer members than the second set of packets, at least some of the packets in the second set of packets to include media information associated with the first session, and, in steps (c) and (e), a corresponding entry to be identified using the network address and session identifier of the first endpoint. As noted, Pruthi et al. appears to teach the use of ATM session identifier alone. (*See* example at ¶¶ 0047 and 0048.)

Dependent claims 34 and 43 require the session monitor to:

determine whether a pair of session entries in the second set of data structures pertain to a common session; and

when the second set of data structures includes a pair of session entries pertaining to a common session, remove the pair of entries from the second set of data structures and adding the pair of session entries to a common session entry in the first set of data structures. Dependent claims 35 and 44 further require, when the at least one of the first endpoint's network address

and session identifier are not in the first and second sets of data structures, the at least one of the first endpoint's network address and session identifier to be added to the second set of data structures. As noted, Pruthi et al. fails to teach the use of first and second sets of data structures to contain network performance information respecting unidentified and identified sessions, respectively. (*See also* dependent claims 36-37, 45-46, 50, and 53.)

Dependent claims 49 and 52 require the first endpoint to transmit at least a second packet to a session monitor when a value of a flag has a first predetermined value. As noted above, the flag indicates whether or not the sending, or second, endpoint already sent a packet to the session monitor. Pruthi, et al., teaches away from this step as it teaches the extraction of packets being exchanged between session endpoints to avoid intruding into the network to evaluate or estimate network performance. According to Pruthi et al., intrusion by introducing additional packets into the network can further degrade performance and is therefore highly undesirable. (¶0008.),

Based upon the foregoing, Applicants believe that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

SHERIDAN ROSS P.C.

By: Douglas Swartz

Douglas W. Swartz
Registration No. 37,739
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: June 13, 2006